51st IEEE Conference on Decision and Control
December 10-13, 2012. Maui, Hawaii, USA

Finite Bisimulations for Switched Linear Systems

Ebru Aydin Gol, Xuchu Ding, Mircea Lazar and Calin Belta

Abstract— **In this paper, we consider the problem of constructing a finite bisimulation quotient for a discrete-time switched linear system in a bounded subset of its state space. Given a set of observations over polytopic subsets of the state space and a switched linear system with stable subsystems, the proposed algorithm generates the bisimulation quotient in a finite number of steps with the aid of sublevel sets of a polyhedral Lyapunov function. Starting from a sublevel set that includes the origin in its interior, the proposed algorithm iteratively constructs the bisimulation quotient for any larger sublevel set. The bisimulation quotient can then be further used for synthesis of the switching law and system verification with respect to specifications given as syntactically co-safe Linear Temporal Logic formulas over the observed polytopic subsets.**

I. INTRODUCTION

In recent years, there has been a trend to bridge the gap between control theory and formal methods. It has been shown that certain classes of dynamical systems can be abstracted to finite transition systems. As a result, model checking and automata games can be used to analyze and control systems with non-trivial dynamics from specifications given as temporal logic formulas.

In this paper, we focus on switched linear systems made of stable subsystems, and show that finite bisimulations can be efficiently constructed within some relevant, bounded subset of the state space. Since the bisimulation quotient preserves all properties that are expressible in frameworks as rich as μ-calculus, and implicitly Computation Tree Logic (CTL) and Linear Temporal Logic (LTL) (see *e.g.,* [1], [2]), it can be readily used for system verification and controller synthesis against such specifications. We show how our method can be used for both controller synthesis and verification from specifications given as arbitrary formulas of a fragment of LTL, called syntactically co-safe LTL (scLTL). For controller synthesis, we find the largest set of initial states and switching sequences such that all system trajectories satisfy a given formula. For verification, we find the largest set of initial states such that all system trajectories satisfy the formula under arbitrary switching.

The concept of constructing a finite quotient of an infinite system has been widely studied, *e.g.,* [3]–[5]. It is known that finite state bisimulation quotients exist only for specific classes of systems (*e.g.,* timed automata [5] and controllable linear systems [3]), and the well known bisimulation algorithm [1] in general does not terminate [6]. Approximately bisimilar finite abstractions for continuous-time switched systems were constructed under incremental stability assumptions in [7]. For piecewise linear systems, guided refinement procedures were employed with the goal of constructing the quotient system for verification of certain properties [4], [6].

We propose to obtain a finite bisimulation quotient of the system in a computationally feasible manner by only considering the system behavior within a relevant state space that does not contain the origin, *i.e.,* in between two positively invariant compact sets that contain the origin. Our approach relies upon the existence of a *polyhedral* Lyapunov function, which is a necessary condition for stability under arbitrary switching, see, e.g., [8]. We propose to partition the state space by using sublevel sets of the Lyapunov function. Such sublevel sets, which are polytopic, allow us to generate the bisimulation quotient incrementally as the abstraction algorithm iterates, with no "holes" in the covered state space. Since we can obtain polytopic sublevel sets of any size from the Lyapunov function, the balance between the size of the abstracted state space and the amount of computation can be easily adjusted and controlled. Starting from the observation that the existence of the Lyapunov function renders the origin asymptotically stable for the switched system, its trajectories can only spend a finite time in the region of interest. As a result, we restrict our attention to LTL specifications that can be satisfied in finite time, such as scLTL formulas.

This paper is an extension of our recent work [9], in which we used polytopic sublevel sets to generate a bisimulation quotient for a discrete autonomous linear system. Another conceptually related work is [10], where n Lyapunov functions were used for the abstraction of n-dimensional continuous-time Morse-Smale systems to timed automata. The abstraction proposed therein is weaker than bisimulation, but it can be used to verify safety properties. While both [10] and this work use sublevel sets for abstraction, the main difference between [10] and this approach comes from the usage of *polyhedral Lyapunov functions*, and therefore different classes of systems for which the methods apply. Our approach removes the need for multiple orthogonal Lyapunov functions, and we argue that it allows for a more tractable implementation since the abstraction of timed automata is expensive by itself [5], and polytopic sublevel sets ensure that the abstraction algorithm requires only polytopic operations.

Due to space limitations, the results in this paper are stated without proofs. The proofs and additional details can be found in [11].

This work was partially supported by the NSF under grants CNS-0834260 and CNS-1035588 and by the ONR under grant MURI N00014-09-1051 at Boston University, and by Veni grant 10230 at Eindhoven University of Technology.

Ebru Aydin Gol (ebru@bu.edu) and Calin Belta (cbelta@bu.edu) are with Boston University. Xuchu Ding (dingx@utrc.utc.com) is with United Technologies Research Center. Mircea Lazar (m.lazar@tue.nl) is with Eindhoven University of Technology.

978-1-4673-2066-5/12/$31.00 ©2012 IEEE

II. PRELIMINARIES

Notation: For a set $\mathcal{S}$, $\mathrm{int}(\mathcal{S})$, $|\mathcal{S}|$, and $2^{\mathcal{S}}$ stand for its interior, cardinality, and power set, respectively. For $\lambda \in \mathbb{R}$ and $\mathcal{S} \subseteq \mathbb{R}^n$, let $\lambda\mathcal{S} := \{\lambda x \mid x \in \mathcal{S}\}$. We use $\mathbb{R}, \mathbb{R}_+, \mathbb{Z}$, and $\mathbb{Z}_+$ to denote the sets of real numbers, non-negative reals, integer numbers, and non-negative integers. For $m, n \in \mathbb{Z}_+$, we use $\mathbb{R}^n$ and $\mathbb{R}^{m\times n}$ to denote the set of column vectors and matrices with n and $m\times n$ real entries. For a vector v or a matrix A, we denote $v^\top$ or $A^\top$ as its transpose, respectively. We use $\|\cdot\|_\infty$ for the infinity norm of a vector or matrix. A *semi-linear* set in $\mathbb{R}^n$ is defined as finite unions, intersections and complements of sets $\{x \in \mathbb{R}^n \mid a^\top x \sim b, \sim \in \{=, <\}\}$, for some $a \in \mathbb{R}^n$ and $b \in \mathbb{R}$.

A. Transition systems and bisimulations

Definition 2.1: A transition system (TS) is a tuple $\mathcal{T} = (Q, \Sigma, \to, \Pi, h)$, where Q is a (possibly infinite) set of states; Σ is a set of inputs; $\to \subseteq Q \times \Sigma \times Q$ is a set of transitions; Π is a finite set of observations; and $h : Q \longrightarrow 2^\Pi$ is an observation map. We denote $x \xrightarrow{\sigma} x'$ if $(x, \sigma, x') \in \to$. We assume $\mathcal{T}$ to be non-blocking, *i.e.,* for each $x \in Q$, there exists $x' \in Q$ and $\sigma \in \Sigma$ such that $x \xrightarrow{\sigma} x'$. An *input word* is defined as an infinite sequence $\boldsymbol{\sigma} = \sigma_0\sigma_1 \ldots$ where $\sigma_k \in \Sigma$ for all $k \in \mathbb{Z}_+$. A *trajectory* of $\mathcal{T}$ produced by an input word $\boldsymbol{\sigma} = \sigma_0\sigma_1 \ldots$ and originating at state x_0 is an infinite sequence $\mathbf{x} = x_0x_1 \ldots$ where $x_k \xrightarrow{\sigma_k} x_{k+1}$ for all $k \in \mathbb{Z}_+$. A trajectory $\mathbf{x}$ generates a word $\mathbf{o} = o_0o_1 \ldots$, where $o_k = h(x_k)$ for all $k \in \mathbb{Z}_+$.

The TS $\mathcal{T}$ is *finite* if $|Q| < \infty$ and $|\Sigma| < \infty$, and *deterministic* if $x \xrightarrow{\sigma} x'$ implies that there does not exist $x'' \neq x'$ such that $x \xrightarrow{\sigma} x''$. Given a set $X \subseteq Q$, we define the set of states $\mathrm{Pre}_{\mathcal{T}}(X, \sigma)$ that reach X in one step when input σ is applied as

$$\mathrm{Pre}_{\mathcal{T}}(X, \sigma) := \{x \in Q \mid \exists x' \in X, x \xrightarrow{\sigma} x'\}. \tag{1}$$

States of a TS can be related by a relation $\sim \subseteq Q \times Q$. For convenience of notation, we denote $x \sim x'$ if $(x, x') \in \sim$. The subset $X \subseteq Q$ is called an *equivalence class* if $x, x' \in X \Leftrightarrow x \sim x'$. We denote by $Q/_\sim$ the set labeling all equivalence classes and define a map $\mathrm{eq} : Q/_\sim \mapsto 2^Q$ such that $\mathrm{eq}(X)$ is the set of states in the equivalence class $X \in Q/_\sim$. We say that a relation $\sim$ is *observation preserving* if for any $x, x' \in Q$, $x \sim x'$ implies that $h(x) = h(x')$. A finite *partition* P of a set $\mathcal{S}$ is a finite collection of sets $P := \{P_i\}_{i\in I}$, such that $\cup_{i\in I} P_i = \mathcal{S}$ and $P_i \cap P_j = \emptyset$ if $i \neq j$. A finite *refinement* of P is a finite partition P' of $\mathcal{S}$ such that for each $P_i \in P'$, there exists $P_j \in P$ such that $P_i \subseteq P_j$.

A partition naturally induces a relation, and an observation preserving relation induces a quotient TS. One can immediately verify that a refinement of an observation preserving partition is also observation preserving.

Definition 2.2: An observation preserving relation $\sim$ of a TS $\mathcal{T} = (Q, \Sigma, \to, \Pi, h)$ induces a *quotient transition system* $\mathcal{T}/_\sim = (Q/_\sim, \Sigma, \to_\sim, \Pi, h_\sim)$, where $Q/_\sim$ is the set labeling all equivalence classes. The transitions of $\mathcal{T}/_\sim$ are defined as $X \xrightarrow{\sigma}_\sim Y$ if and only if there exists $x \in \mathrm{eq}(X)$ and $x' \in \mathrm{eq}(Y)$ such that $x \xrightarrow{\sigma} x'$. The observation map is defined as $h_\sim(X) := h(x)$, where $x \in \mathrm{eq}(X)$.

Definition 2.3: Given a TS $\mathcal{T} = (Q, \Sigma, \to, \Pi, h)$, a relation $\sim$ is a bisimulation relation of $\mathcal{T}$ if (1) $\sim$ is observation preserving; (2) for any $x_1, x_2 \in Q, \sigma \in \Sigma$, if $x_1 \sim x_2$ and $x_1 \xrightarrow{\sigma} x_1'$, there exists $x_2' \in Q$ such that $x_2 \xrightarrow{\sigma} x_2'$ and $x_1' \sim x_2'$.

If $\sim$ is a bisimulation, then the quotient transition system $\mathcal{T}/_\sim$ is called a *bisimulation quotient* of $\mathcal{T}$. In this case, $\mathcal{T}$ and $\mathcal{T}/_\sim$ are said to be *bisimilar*. Bisimulations preserve properties expressed in temporal logics such as LTL, CTL and μ-calculus [1], [2].

B. Polyhedral Lyapunov functions

Consider an autonomous discrete-time system,

$$x_{k+1} = \Phi(x_k), \quad k \in \mathbb{Z}_+, \tag{2}$$

where $x_k \in \mathbb{R}^n$ is the state at the discrete-time instant k and $\Phi : \mathbb{R}^n \mapsto \mathbb{R}^n$ is an arbitrary map with $\Phi(0) = 0$. Given a state $x \in \mathbb{R}^n$, $x' := \Phi(x)$ is called a *successor* state of x.

Definition 2.4: Let $\lambda \in [0, 1]$. We call a set $\mathcal{P} \subseteq \mathbb{R}^n$ λ-*contractive* (shortly, contractive) if for all $x \in \mathcal{P}$ it holds that $\Phi(x) \in \lambda\mathcal{P}$. For $\lambda = 1$, we call $\mathcal{P}$ a *positively invariant* set.

Theorem 2.1: Let $\mathcal{X}$ be a positively invariant set for (2) with $0 \in \mathrm{int}(\mathcal{X})$. Furthermore, let $\alpha_1, \alpha_2 \in \mathcal{K}_\infty$, $\rho \in (0, 1)$ and $V : \mathbb{R}^n \mapsto \mathbb{R}_+$ such that:

$$\alpha_1(\|x\|) \leq V(x) \leq \alpha_2(\|x\|), \forall x \in \mathcal{X}, \tag{3}$$

$$V(\Phi(x)) \leq \rho V(x), \forall x \in \mathcal{X}. \tag{4}$$

Then system (2) is asymptotically stable in $\mathcal{X}$.

The proof of Thm. 2.1 can be found in [12], [13].

Definition 2.5: A function $V : \mathbb{R}^n \mapsto \mathbb{R}_+$ is called a *Lyapunov function* (LF) in $\mathcal{X}$ if it satisfies (3) and (4). If $\mathcal{X} = \mathbb{R}^n$, then V is called a *global Lyapunov function*.

The parameter ρ is called the *contraction rate* of V. For any $\Gamma > 0$, $\mathcal{P}_\Gamma := \{x \in \mathbb{R}^n \mid V(x) \leq \Gamma\}$ is called a *sublevel set* of V.

For the remainder of this paper we consider LFs defined using the infinity norm, i.e.,

$$V(x) = \|Lx\|_\infty, \quad L \in \mathbb{R}^{l\times n}, l \geq n, l \in \mathbb{Z}_+, \tag{5}$$

where L has full-column rank. Notice that infinity norm Lyapunov functions are a particular type of polyhedral Lyapunov functions. We opted for this type of function to simplify the exposition but in fact, the proposed abstraction method applies to general polyhedral Lyapunov functions defined by Minkowski (gauge) functions of polytopes in $\mathbb{R}^n$ with the origin in their interior.

Proposition 2.1: Suppose that $L \in \mathbb{R}^{l\times n}$ has full-column rank and V as defined in (5) is a global LF for system (2) with contraction rate $\rho \in (0, 1)$. Then for all $\Gamma > 0$ it holds that $\mathcal{P}_\Gamma$ is a polytope and $0 \in \mathrm{int}(\mathcal{P}_\Gamma)$. Moreover, if $\Phi(x)$ takes values arbitrarily from a set $\{Ax \mid A \in \mathcal{A}\}$ for some polyhedral set $\mathcal{A} \subseteq \mathbb{R}^{n\times n}$, then *for all* $\Gamma > 0$ it holds that $\mathcal{P}_\Gamma$ is a ρ-contractive polytope for (2).

III. PROBLEM FORMULATION

In this paper, we consider discrete-time switched linear systems, *i.e.,*

$$x_{k+1} = A_{\boldsymbol{\sigma}(k)} x_k, \quad \boldsymbol{\sigma}(k) \in \Sigma, k \in \mathbb{Z}_+, \tag{6}$$

where $\boldsymbol{\sigma} : \mathbb{Z}_+ \to \Sigma$ is a switching sequence that selects the active subsystem from a finite index set Σ and $A_i \in \mathbb{R}^{n\times n}$ is a strictly stable (i.e., Schur) matrix for all $i \in \Sigma$. We assume that a global polyhedral Lyapunov function (LF) of the form (5) with contraction rate $\rho \in (0, 1)$ is known for system (6).

Let $\mathcal{X}$ be a polytope $\mathcal{X} := \{x \mid \|Lx\|_\infty \leq \Gamma_\mathcal{X}\}$ and $\mathcal{D}$ be a polytope $\mathcal{D} := \{x \mid \|Lx\|_\infty \leq \Gamma_\mathcal{D}\}$, where L corresponds to the polytopic LF (5) of system (6) and we assume that $0 < \Gamma_\mathcal{D} < \Gamma_\mathcal{X}$. Note that $\mathcal{D} \subset \mathcal{X}$ and $0 \in \text{int}(\mathcal{D}) \subset \text{int}(\mathcal{X})$. We call $\mathcal{X}$ the working set and $\mathcal{D}$ the target set. We are interested in synthesis of control strategies and verification of the system behavior within $\mathcal{X}$ with respect to polytopic regions in the state space, until the target set $\mathcal{D}$ is reached (since $\mathcal{D}$ is positively invariant, the system trajectory will be confined within $\mathcal{D}$ after $\mathcal{D}$ is reached).

We assume that there exists a set $\mathcal{R}$ of polytopes indexed by a finite set R, *i.e.,* $\mathcal{R} := \{\mathcal{R}_i\}_{i\in R}$, where $\mathcal{R}_i \subseteq \mathcal{X} \setminus \mathcal{D}$ for all $i \in R$, and $\mathcal{R}_i \cap \mathcal{R}_j = \emptyset$ for any $i \neq j$. The set $\mathcal{R}$ represents regions of interest in the relevant state space, and the polytopes in $\mathcal{R}$ are considered as observations of (6). Therefore, informally, a trajectory of (6) $x_0x_1\ldots$ produces an infinite sequence of observations $o_0o_1\ldots$, such that o_i is the index of the polytope in $\mathcal{R}$ visited by state x_i, or $o_i = \emptyset$ if x_i is in none of the polytopes.

Example 3.1: Consider a system as in (6), $\Sigma = \{1, 2\}$, $A_1 = \begin{pmatrix} -0.65 & 0.32 \\ -0.42 & -0.92 \end{pmatrix}$ and $A_2 = \begin{pmatrix} 0.65 & 0.32 \\ -0.42 & -0.92 \end{pmatrix}$. The algorithm proposed in [8] is employed to construct a global polytopic LF of the form (5), where

$$L = \begin{pmatrix} -0.0625 & 0.6815 & 0.9947 & 0.9947 \\ 1 & 1 & 0.6868 & -0.0678 \end{pmatrix}^\top,$$

and $\rho = 0.94$. We chose $\Gamma_\mathcal{X} = 10$ and $\Gamma_\mathcal{D} = 5.063$. (see Fig. 1 for polytopes $\mathcal{X}$, $\mathcal{D}$, and a set of polytopes $\mathcal{R}$.)

The semantics of the system can be formalized through an embedding of (6) into a transition system, as follows.

Definition 3.1: Let $\mathcal{X}$, $\mathcal{D}$, and $\mathcal{R} = \{\mathcal{R}_i\}_{i\in R}$ be given. The embedding transition system for (6) is a transition system $\mathcal{T}_e = (Q_e, \Sigma, \to_e, \Pi, h_e)$ where

- $Q_e = \{x \in \mathbb{R}^n \mid x \in \mathcal{X}\}$;
- Σ is the same as the index set given in Eqn (6);
- 1) If $x \in \mathcal{X} \setminus \mathcal{D}$, then $x \xrightarrow{\sigma}_e x'$ if and only if $x' = A_\sigma x$, *i.e.,* x' is the state at the next time-step after applying the dynamics of (6) at x when subsystem σ is active;
  2) If $x \in \mathcal{D}$, $x \xrightarrow{\sigma}_e x$ for all $\sigma \in \Sigma$ (since the target set $\mathcal{D}$ is already reached, we consider the behavior of the system thereafter no longer relevant);
- $\Pi = R \cup \{\Pi_\mathcal{D}\}$, *i.e.,* the set of observations is the set of labels of regions, plus the label $\Pi_\mathcal{D}$ for $\mathcal{D}$;
- 1) $h_e(x) := i$ if and only if $x \in \mathcal{R}_i$;
  2) $h_e(x) := \emptyset$ if and only if $x \in \mathcal{X} \setminus (\mathcal{D} \cup \bigcup_{i\in R} \mathcal{R}_i)$;
  3) $h_e(x) := \Pi_\mathcal{D}$ if and only if $x \in \mathcal{D}$.

Note that $\mathcal{T}_e$ is deterministic and it has an infinite number of states. Moreover, $\mathcal{T}_e$ exactly captures the system dynamics under (6) in the relevant state space $\mathcal{X} \setminus \mathcal{D}$, since a transition of $\mathcal{T}_e$ naturally corresponds to the evolution of the discrete-time system in one time-step. Indeed, within $\mathcal{X} \setminus \mathcal{D}$, the trajectory of $\mathcal{T}_e$ produced by an input word $\boldsymbol{\sigma}$ from a state $x \in \mathcal{X} \setminus \mathcal{D}$ is exactly the same as the trajectory of system (6) from x under the switching sequence $\boldsymbol{\sigma}$. The state space of $\mathcal{T}_e$ (which is the working set $\mathcal{X}$) can be naturally partitioned as

$$P_\mathcal{X} := \left\{ \{\mathcal{R}_i\}_{i\in R}, \mathcal{X} \setminus (\mathcal{D} \cup \bigcup_{i\in R} \mathcal{R}_i), \mathcal{D} \right\}. \tag{7}$$

The relation induced from partition $P_\mathcal{X}$ is observation preserving (see Sec. II-A). We now formulate the main problem considered in this paper.

Problem 3.1: Let a system (6) with a polyhedral Lyapunov function of the form (5), sets $\mathcal{X}$, $\mathcal{D}$ and $\{\mathcal{R}_i\}_{i\in R}$ be given. Compute a finite observation preserving partition P such that its induced relation $\sim$ is a bisimulation of the embedding transition system $\mathcal{T}_e$, and obtain the corresponding bisimulation quotient $\mathcal{T}_e/\!\sim$.

IV. GENERATING THE BISIMULATION QUOTIENT

Starting from a polyhedral Lyapunov function $V(x) = \|Lx\|_\infty$ with a contraction rate $\rho = (0, 1)$ as described in Sec. II-B for system (6), we first generate a sequence of polytopic sublevel sets of the form $\mathcal{P}_\Gamma := \{x \in \mathbb{R}^n \mid \|Lx\|_\infty \leq \Gamma\}$ as follows. Recall that $\mathcal{X} = \mathcal{P}_{\Gamma_\mathcal{X}}$ and $\mathcal{D} = \mathcal{P}_{\Gamma_\mathcal{D}}$ for some $0 < \Gamma_\mathcal{D} < \Gamma_\mathcal{X}$. We define a finite sequence $\bar{\Gamma} := \Gamma_0, \ldots, \Gamma_N$, where

$$\Gamma_{i+1} = \rho^{-1}\Gamma_i, \quad i = 0, \ldots, N-2, \tag{8}$$

$\Gamma_0 := \Gamma_\mathcal{D}$, $\Gamma_N := \Gamma_\mathcal{X}$, and $N := \arg\min_N\{\rho^{-N}\Gamma_0 \mid \rho^{-N}\Gamma_0 \geq \Gamma_\mathcal{X}\}$. This choice of N guarantees that $\mathcal{P}_{\Gamma_{N-1}}$ is the largest sublevel set defined via (8) that is a subset of $\mathcal{X}$. Since Γ_N is exactly $\Gamma_\mathcal{X}$, $\mathcal{P}_{\Gamma_N}$ is exactly $\mathcal{X}$.

The sequence $\bar{\Gamma}$ generates a sequence of sublevel sets $\bar{\mathcal{P}}_\Gamma := \mathcal{P}_{\Gamma_0}, \ldots, \mathcal{P}_{\Gamma_N}$. From the definition of the sublevel sets and $\bar{\Gamma}$, we have that

$$\mathcal{P}_{\Gamma_0} \subset \ldots \subset \mathcal{P}_{\Gamma_N}. \tag{9}$$

Next, we define a *slice* of the state space as follows:

$$\mathcal{S}_i := \mathcal{P}_{\Gamma_i} \setminus \mathcal{P}_{\Gamma_{i-1}}, \quad i = 1, \ldots, N. \tag{10}$$

For convenience, we also denote $\mathcal{S}_0 := \mathcal{P}_{\Gamma_0}$ (although $\mathcal{S}_0$ is not a slice in between two sublevel sets). We immediately see that the sets $\{\mathcal{S}_i\}_{i=0,\ldots,N}$ form a partition of $\mathcal{X}$. Note that the slices are bounded semi-linear sets (see Sec. II).

Example 4.1: Consider the system given in Example 3.1 and $N = 11$ in Eqn. (8). The polytopic sublevel sets $\bar{\mathcal{P}}_\Gamma := \mathcal{P}_{\Gamma_0}, \ldots, \mathcal{P}_{\Gamma_{11}}$ are shown in in Fig. 1.

Proposition 4.1: Assume that the set of slices $\{\mathcal{S}_i\}_{i=0,\ldots,N}$ is obtained from a sequence $\bar{\Gamma}$ satisfying (8). Given a state x in the i-th slice, *i.e.,* $x \in \mathcal{S}_i$, where $1 \leq i \leq N$, its successor state ($x' = A_\sigma x$, $\sigma \in \Sigma$) satisfies $x' \in \mathcal{S}_j$ for some $j < i$.

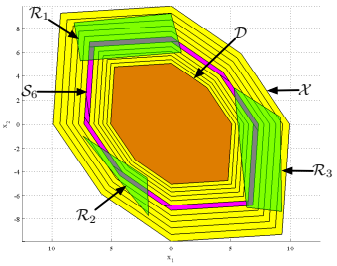


Fig. 1: An example in $\mathbb{R}^2$ of the working set $\mathcal{X}$, the target set $\mathcal{D}$ (in brown), a set of observational relevant polytopes $\mathcal{R} = \{\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3\}$ (in transparent green), sublevel sets with $N = 11$ and one slice $\mathcal{S}_6$ (in purple).

We now present the abstraction algorithm (see Alg. 1) that computes the bisimulation quotient. In Alg. 1, we make use of two procedures `ComputePre` and `RefineUpdate`, which will be further explained below. The main idea is to start with $P_{\mathcal{X}}$ (Eqn. (7)), refine the partition according to $\{\mathcal{S}_i\}_{i=0,\dots,N}$ to guarantee that it is a refinement to both $P_{\mathcal{X}}$ as in (7) and $\{\mathcal{S}_i\}_{i=0,\dots,N}$, and then iteratively refine according to the Pre operator (see Eqn. 1). The first step, starting with $P_{\mathcal{X}}$, is necessary so that the partition is observation preserving. The second step guarantees that each element in the partition is included in a slice. The third step allows us to ensure that at iteration i of the algorithm, the bisimulation quotient for states within $\mathcal{P}_{\Gamma_i}$ is completed.

Algorithm 1 Abstraction algorithm

Input: System dynamics (6), polytopic LF $V(x) = \|Lx\|_\infty$ with a contractive rate ρ, sets $\mathcal{X}$, $\mathcal{D}$ and $\{\mathcal{R}_i\}_{i\in R}$.
Output: $\mathcal{T}_e/_\sim$ as a bisimulation quotient of the embedding transition system $\mathcal{T}_e$ and the corresponding observation preserving partition P.

Obtain $P_{\mathcal{X}}$ as in (7).
Generate the sequence of sublevel sets $\bar{\mathcal{P}}_\Gamma = \mathcal{P}_{\Gamma_0}, \dots, \mathcal{P}_{\Gamma_N}$ and slices $\mathcal{S}_0, \dots, \mathcal{S}_N$ as defined in(10).
Set $P_0 = \{\emptyset \subset \tilde{\mathcal{P}}_1 \cap \tilde{\mathcal{P}}_2 \,|\, \tilde{\mathcal{P}}_1 \in P_{\mathcal{X}}, \tilde{\mathcal{P}}_2 \in \{\mathcal{S}_i\}_{i=0,\dots,N}\}$.
Initialize $\mathcal{T}_e/_{\sim_0}$ by setting $Q_e/_{\sim_0}$ as the set labeling P_0. Set transitions only for the state $q \in Q_e/_{\sim_0}$ where $\mathrm{eq}(q) = \mathcal{S}_0 = \mathcal{D}$ with $q \xrightarrow{\sigma}_{\sim_0} q$ for all $\sigma \in \Sigma$.
for each $i = 0, \dots, N-1$ **do**
  Set $\mathcal{T}_e/_{\sim_{i+1}} = \mathcal{T}_e/_{\sim_i}$ **and** $P_{i+1} = P_i$.
  for each $q \in Q_e/_{\sim_i}$ where $\mathrm{eq}(q) \subseteq \mathcal{S}_i$ **do**
    for each $\sigma \in \Sigma$ **do**
      Find $\tilde{\mathcal{P}} = \texttt{ComputePre}(\mathrm{eq}(q), \sigma)$.
      Set $[P_{i+1}, \mathcal{T}_e/_{\sim_{i+1}}] = \texttt{RefineUpdate}$ $(P_{i+1}, \mathcal{T}_e/_{\sim_{i+1}}, \tilde{\mathcal{P}}, \sigma, q)$.
    end for
  end for
end for
Return $\mathcal{T}_e/_{\sim_N}$ and P_N as a solution to Prob. 3.1.

The procedure $\texttt{ComputePre}(\tilde{\mathcal{P}}, \sigma)$ takes as input $\tilde{\mathcal{P}}$, which is a bounded semi-linear set (*e.g.,* a slice), and $\sigma \in \Sigma$, which is the switching input, and returns the set $\mathrm{Pre}_{\mathcal{T}_e}(\tilde{\mathcal{P}}, \sigma)$. If $\tilde{\mathcal{P}}$ is a polytope, then $\mathrm{Pre}_{\mathcal{T}_e}(\tilde{\mathcal{P}}, \sigma)$ is computed as

$$\mathrm{Pre}_{\mathcal{T}_e}(\tilde{\mathcal{P}}, \sigma) = \{x \in \mathbb{R}^n \,|\, H_{\tilde{\mathcal{P}}} A_\sigma x \le h_{\tilde{\mathcal{P}}}\}, \qquad (11)$$

where $\tilde{\mathcal{P}} = \{x \in \mathbb{R}^n \,|\, H_{\tilde{\mathcal{P}}} x \le h_{\tilde{\mathcal{P}}}\}$. In general, if $\tilde{\mathcal{P}}$ is a semi-linear set, then $\mathrm{Pre}_{\mathcal{T}_e}(\tilde{\mathcal{P}}, \sigma)$ is also a semi-linear set and it can be computed via quantifier elimination [14]. In particular, $\mathrm{Pre}_{\mathcal{T}_e}(\tilde{\mathcal{P}}, \sigma)$ for a bounded semi-linear set $\tilde{\mathcal{P}}$ can be computed via a convex decomposition and repeated applications of (11). This computation is discussed in more detail in [9]. Note that $\texttt{ComputePre}(\tilde{\mathcal{P}}, \sigma)$ only requires polytopic operations.

The procedure $\texttt{RefineUpdate}(P, \mathcal{T}, \tilde{\mathcal{P}}, \sigma, q)$ (outlined in Alg. 2) refines a partition P with respect to set $\tilde{\mathcal{P}}$, where $\tilde{\mathcal{P}} = \texttt{ComputePre}(\mathrm{eq}(q), \sigma)$. It then updates $\mathcal{T}$. If P consists of only bounded semi-linear sets and $\tilde{\mathcal{P}}$ is a semi-linear set, then the resulting refinement P^+ consists of only bounded semi-linear sets. This fact allows us to always use $\texttt{ComputePre}(\tilde{\mathcal{P}}, \sigma)$.

Algorithm 2 $[P^+, \mathcal{T}^+] = \texttt{RefineUpdate}(P, \mathcal{T}, \tilde{\mathcal{P}}, \sigma, q)$

Input: A TS $\mathcal{T} = (Q, \Sigma, \to, \Pi, h)$, a partition P where $\mathrm{eq}(q') \in P$ for all $q' \in Q$, and $\tilde{\mathcal{P}} = \texttt{ComputePre}(\mathrm{eq}(q), \sigma)$ for some $q \in Q$, $\sigma \in \Sigma$.
Output: P^+ is a finite refinement of P with respect to $\tilde{\mathcal{P}}$, $\mathcal{T}^+$ is a TS updated from $\mathcal{T}$.

Set $P^+ = P$ **and** $\mathcal{T}^+ = \mathcal{T}$.
for all $q' \in Q^+$ such that $\mathrm{eq}(q') \cap \tilde{\mathcal{P}} \neq \emptyset$ **do**
  Replace q' in Q^+ by $\{q_1, q_2\}$ and set $\mathrm{eq}(q_1) = \mathrm{eq}(q') \cap \tilde{\mathcal{P}}$, $\mathrm{eq}(q_2) = \mathrm{eq}(q') \setminus \tilde{\mathcal{P}}$.
  Replace $\mathrm{eq}(q')$ in P^+ by $\{\mathrm{eq}(q_1), \mathrm{eq}(q_2)\}$.
  Replace each $(q', \sigma', q'') \in \to^+$ by $\{(q_i, \sigma', q'')\}_{i=1,2}$.
  Add transition (q_1, σ, q) to $\to^+$.
end for

The correctness of Alg. 1 will be shown by an inductive argument. Given a sublevel set $\mathcal{P}_{\Gamma_i}$ and a partition P_i as obtained in Alg. 1, we define $\tilde{P}_i$ as

$$\tilde{P}_i := \{\tilde{\mathcal{P}} \in P_i \,|\, \tilde{\mathcal{P}} \subseteq \mathcal{P}_{\Gamma_i}\}. \qquad (12)$$

From Alg. 1, we see that P_0 partitions all the slices, and since P_i is a finite refinement of P_0, we can directly see that $\tilde{P}_i$ is a partition of $\mathcal{P}_{\Gamma_i}$. Let us define an embedding transition system $\mathcal{T}_e(i)$ as a subset of $\mathcal{T}_e$ with set of states $\{x \in Q_e \,|\, x \in \mathcal{P}_{\Gamma_i}\}$ and let us state the following result.

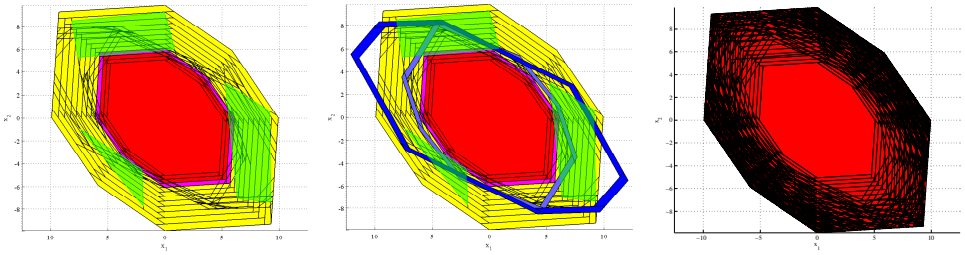
Proposition 4.2: At the completion of the i-th iteration (of the outer loop) of Alg. 1 (where P_{i+1} is obtained), if $\sim_i$ induced by $\tilde{P}_i$ as defined in (12) is a bisimulation of $\mathcal{T}_e(i)$, then $\sim_{i+1}$ induced by $\tilde{P}_{i+1}$ is a bisimulation of $\mathcal{T}_e(i+1)$.

Theorem 4.1: Alg. 1 returns a solution to Prob. 3.1 in finite time.

Example 4.2: Alg. 1 is applied on the same setting as in Example 4.1 to compute the bisimulation quotient. P_3 and P_{11} are shown in Fig. 2.

V. TEMPORAL LOGIC SYNTHESIS AND VERIFICATION

After we obtain a bisimulation quotient for system (6), we can solve verification and controller synthesis problems from temporal logic specifications such as CTL*, CTL and LTL. The asymptotic stability assumption implies that all trajectories of (6) sink in $\mathcal{D}$. For this reason, we will focus on syntactically co-safe fragment of LTL, which includes all specifications of LTL where satisfactions of trajectories can be determined by a finite prefix. Since we are interested in the behavior of (6) until $\mathcal{D}$ is reached, scLTL is sufficiently rich as the specification language.



(a) (b) (c)

Fig. 2: The observed regions are shown in transparent green in (a) and (b). (a) At the end of the third iteration ($i = 2$), the bisimulation quotient for states within $\mathcal{P}_{\Gamma_3}$ is completed, which are shown in red and purple. In the forth iteration, the states within $\mathcal{P}_{\Gamma_{11}} \setminus \mathcal{P}_{\Gamma_3}$ will be partitioned according to $\mathrm{Pre}_{\mathcal{T}_e}(\tilde{\mathcal{P}}, \sigma), \tilde{\mathcal{P}} \in \mathcal{S}_3$. (b) $\mathcal{S}_3$ is shown in purple, and $\mathrm{Pre}_{\mathcal{T}_e}(\mathcal{S}_3, 1)$ and $\mathrm{Pre}_{\mathcal{T}_e}(\mathcal{S}_3, 2)$ are shown in light and dark blue. (c) At the last iteration where $i = 10$, the algorithm is completed. The state space covered by the bisimulation quotient is shown in red, covering all of $\mathcal{X}$.

A detailed description of the syntax and semantics of scLTL is beyond the scope of this paper and can be found in, for example, [15], [16]. Roughly, an scLTL formula is built up from a set of atomic propositions Π, Boolean operators $\neg$ (negation), $\vee$ (disjunction), $\wedge$ (conjunction), $\Rightarrow$ (implication) and temporal operators X (next), U (until) and F (eventually). The semantics of scLTL formulas is given over infinite words $\mathbf{o} = o_0 o_1 \ldots$, where $o_i \in 2^{\Pi}$ for all i. We write $\mathbf{o} \vDash \phi$ if the word $\mathbf{o}$ satisfies the scLTL formula ϕ. We say a trajectory $\mathbf{q}$ of a transition system $\mathcal{T}$ satisfies scLTL formula ϕ, if the word generated by $\mathbf{q}$ satisfies ϕ.

Example 5.1: Again, consider the setting in Example 3.1 with $\mathcal{R} = \{\mathcal{R}_i\}_{i=\{1,2,3\}}$. We now consider a specification in scLTL over $\{\mathcal{R}_1, \mathcal{R}_2, \mathcal{R}_3, \Pi_{\mathcal{D}}\}$. For example, the specification *"A system trajectory never visits $\mathcal{R}_2$ and eventually visits $\mathcal{R}_1$. Moreover, if it visits $\mathcal{R}_3$ then it must not visit $\mathcal{R}_1$ at the next time step"* can be translated to a scLTL formula:

$$\phi := (\neg \mathcal{R}_2 \,\mathsf{U}\, \Pi_{\mathcal{D}}) \wedge \mathsf{F}\, \mathcal{R}_1 \wedge ((\mathcal{R}_3 \Rightarrow \mathsf{X} \neg \mathcal{R}_1) \,\mathsf{U}\, \Pi_{\mathcal{D}}) \quad (13)$$

A. Synthesis of switching strategies

In this section, we assume that we can choose the dynamics A_σ, $\sigma \in \Sigma$ to be applied at each step k.

Problem 5.1: Consider system (6) with a polyhedral Lyapunov function in the form of (5), sets $\mathcal{X}$, $\mathcal{D}$ and $\{\mathcal{R}_i\}_{i \in R}$, and a scLTL formula ϕ over $R \cup \{\Pi_{\mathcal{D}}\}$. Find the largest set $\mathcal{X}^S \subseteq \mathcal{X}$ and a function $\Omega : \mathcal{X}^S \mapsto \Sigma^*$ such that the trajectory of system (6) initiated from a state $x_0 \in \mathcal{X}^S$ under the switching sequence $\Omega(x_0)$ satisfies ϕ.

As a switched system is deterministic, it produces a unique trajectory for a given initial state and switching sequence. This fact allows us to provide a solution to Problem 5.1 as an assignment of a switching sequence to each initial state. Our solution to Prob. 5.1 proceeds by finding a bisimulation quotient $\mathcal{T}_e/_\sim$ of the embedding transition system $\mathcal{T}_e$ using Alg. 1. Then we translate ϕ to a Finite State Automaton (FSA), defined below.

Definition 5.1: A deterministic finite state automaton (FSA) is a tuple $\mathcal{A} = (S_{\mathcal{A}}, S_{\mathcal{A}0}, \Sigma, \delta_{\mathcal{A}}, F_{\mathcal{A}})$ where $S_{\mathcal{A}}$ is a finite set of states; $S_{\mathcal{A}0} \subseteq S_{\mathcal{A}}$ is a set of initial states; Σ is an input alpabet; $\delta_{\mathcal{A}} : S_{\mathcal{A}} \times \Sigma \to S_{\mathcal{A}}$ is a transition function; and $F_{\mathcal{A}} \subseteq S_{\mathcal{A}}$ is a set of final states.

A word $\boldsymbol{\sigma} = \sigma_0 \ldots \sigma_{d-1}$ over Σ generates a trajectory $s_0 \ldots s_d$, where $s_0 \in S_{\mathcal{A}0}$ and $\delta(s_i, \sigma_i) = s_{i+1}$ for all $i = 0, \ldots, d-1$. $\mathcal{A}$ accepts word $\boldsymbol{\sigma}$ if $s_d \in F_{\mathcal{A}}$.

For any scLTL formula ϕ over Π, there exists a FSA $\mathcal{A}$ with input alphabet 2^{Π} that accepts the prefixes of all and only the satisfying words [15], [17].

Definition 5.2: Given a transition system $\mathcal{T} = (Q, \Sigma, \to, \Pi, h)$ and a FSA $\mathcal{A} = (S_{\mathcal{A}}, S_{\mathcal{A}0}, 2^{\Pi}, \delta_{\mathcal{A}}, F_{\mathcal{A}})$, their product automaton, denoted by $\mathcal{PA} = \mathcal{T} \times \mathcal{A}$, is a tuple $\mathcal{PA} = (S_{\mathcal{PA}}, S_{\mathcal{PA}0}, \Sigma, \to_{\mathcal{PA}}, F_{\mathcal{PA}})$ where $S_{\mathcal{PA}} = Q \times S_{\mathcal{A}}$; $S_{\mathcal{PA}0} = Q \times S_{\mathcal{A}0}$; $\to_{\mathcal{PA}} \subseteq S_{\mathcal{PA}} \times \Sigma \times S_{\mathcal{PA}}$ is the set of transitions, defined by: $((q, s), \sigma, (q', s')) \in \to_{\mathcal{PA}}$ iff $q \xrightarrow{\sigma} q'$ and $\delta_{\mathcal{A}}(s, h(q)) = s'$; and $F_{\mathcal{PA}} = Q \times F_{\mathcal{A}}$. We denote $s_{\mathcal{PA}} \xrightarrow{\sigma}_{\mathcal{PA}} s'_{\mathcal{PA}}$ if $(s_{\mathcal{PA}}, \sigma, s'_{\mathcal{PA}}) \in \to_{\mathcal{PA}}$. A trajectory $\mathbf{p} = (q_0, s_0) \ldots (q_d, s_d)$ of $\mathcal{PA}$ produced by input word $\boldsymbol{\sigma} = \sigma_0 \ldots \sigma_{d-1}$ is a finite sequence such that $(q_0, s_0) \in S_{\mathcal{PA}0}$ and $(q_k, s_k) \xrightarrow{\sigma_k}_{\mathcal{PA}} (q_{k+1}, s_{k+1})$ for all $k = 0, \ldots, d-1$. $\mathbf{p}$ is called accepting if $(q_d, s_d) \in F_{\mathcal{PA}}$.

By the construction of $\mathcal{PA}$ from $\mathcal{T}$ and $\mathcal{A}$, $\mathbf{p}$ produced by $\boldsymbol{\sigma}$ is accepting if and only if $\mathbf{q} = \gamma_{\mathcal{T}}(\mathbf{p})$ satisfies the scLTL formula corresponding to $\mathcal{A}$ [16], where $\gamma_{\mathcal{T}}(\mathbf{p})$ is the projection of a trajectory $\mathbf{p}$ of $\mathcal{PA}$ onto $\mathcal{T}$ by simply removing the automaton part of the state in $s_{\mathcal{PA}} \in S_{\mathcal{PA}}$.

We construct the product $\mathcal{PA}$ between the quotient transition system $\mathcal{T}_e/_\sim$ obtained from Alg. 1 and FSA $\mathcal{A}$ corresponding to specification formula ϕ. By performing a graph search on $\mathcal{PA}$, we can find the largest subset $S^S_{\mathcal{PA}}$ of $S_{\mathcal{PA}}$ and a feedback control function $\Omega_{\mathcal{PA}} : S^S_{\mathcal{PA}} \mapsto \Sigma$ such that the trajectories of $\mathcal{PA}$ originating in $S^S_{\mathcal{PA}}$ in closed loop with $\Omega_{\mathcal{PA}}$ reach $F_{\mathcal{PA}}$. Then, we define the set of satisfying initial states of system (6) from $S^S_{\mathcal{PA}}$ as

$$\mathcal{X}^S = \{\mathrm{eq}(q) \mid (q, s) \in (S_{\mathcal{PA}0} \cap S^S_{\mathcal{PA}})\}. \quad (14)$$

Since $\mathcal{PA}$ is deterministic, $\Omega_{\mathcal{PA}}$ defines a unique input word for each $(q_0, s_0) \in S^S_{\mathcal{PA}}$. Moreover, an input word of $\mathcal{PA}$ directly maps to a switching sequence for system (6). Formally, the switching sequence $\Omega : \mathcal{X}^S \mapsto \Sigma^*$ is obtained by "projecting" $\Omega_{\mathcal{PA}}$ from $\mathcal{PA}$ to $\mathcal{T}$ as follows:

$$\Omega(x) = \Omega_{\mathcal{PA}}((q_0, s_0)) \ldots \Omega_{\mathcal{PA}}((q_{d-1}, s_{d-1})), \quad (15)$$

where $x \in eq(q_0)$, $s_0 \in S_{\mathcal{A}0}$, $(q_i, s_i) \xrightarrow{\Omega_{\mathcal{PA}}((q_i, s_i))}_{\mathcal{PA}} (q_{i+1}, s_{i+1})$, for each $i = 0, \ldots, d-1$ and $(q_d, s_d) \in F_{\mathcal{PA}}$.

Proposition 5.1: $\mathcal{X}^S$ as defined in Eqn. (14) and function Ω as defined in Eqn. (15) solve Prob. 5.1.

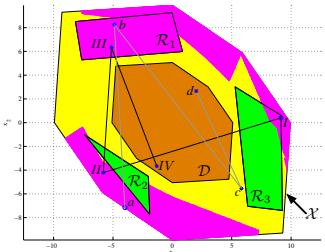


Fig. 3: $\mathcal{X}^S$ is shown in purple. $\mathcal{X}$, $\mathcal{D}$, $\{\mathcal{R}_i\}_{i\in R}$ and two sample trajectories are indicated by their labels.

Example 5.2: For specification ϕ in (13), we obtained the solution to Prob. 5.1. The FSA has 6 states and the quotient TS obtained from Alg. 1 has 9677 states. The set of initial states $\mathcal{X}^S$ is shown in Fig. 3.

B. Verification under arbitrary switching

Problem 5.2: Consider system (6) with a polyhedral Lyapunov function in the form of (5), sets $\mathcal{X}$, $\mathcal{D}$ and $\{\mathcal{R}_i\}_{i\in R}$, and a scLTL formula ϕ over $R\cup\{\Pi_{\mathcal{D}}\}$. Find the largest set $\mathcal{X}^{AS}\subseteq\mathcal{X}$ such that all trajectories of system (6) originating in $\mathcal{X}^{AS}$ satisfy ϕ under arbitrary switching.

Note that system (6) under arbitrary switching is uncontrolled and non-deterministic, *i.e.*, at every time-step a subsystem is arbitrarily chosen from the set Σ. Therefore, we define an embedding transition system $\mathcal{T}_e^A=\{Q_e,\Sigma^A,\rightarrow_e^A,h_e\}$ for the arbitrary switching setup from the embedding transition system $\mathcal{T}_e=\{Q_e,\Sigma,\rightarrow_e,h_e\}$ (Def. 3.1) by adapting the input set and the set of transitions as follows:

- $\Sigma^A=\{\epsilon\}$,
- $\rightarrow_e^A=\{(q,\epsilon,q')\,|\,\exists\sigma\in\Sigma,(q,\sigma,q')\in\rightarrow_e\}$.

We denote $q\rightarrow_e^A q'$ if $(q,\epsilon,q')\in\rightarrow_e^A$. We use ϵ as a "dummy" input because the transitions of $\mathcal{T}_e^A$ are not controlled. Note that $\mathcal{T}_e^A$ is infinite and non-deterministic. Moreover, $\mathcal{T}_e^A$ exactly captures dynamics of system (6) under arbitrary switching in the relevant state space $\mathcal{X}\setminus\mathcal{D}$.

Our solution to Prob 5.2 parallels the solution we proposed for Prob. 5.1. We first convert the bisimulation quotient $\mathcal{T}_e/\sim\,=\{Q_e/\sim,\Sigma,\rightarrow_e/\sim,h_e/\sim\}$ of $\mathcal{T}_e$ obtained from Alg. 1 to $\mathcal{T}_e^A/\sim\,=\{Q_e/\sim,\Sigma^A,\rightarrow_e^A/\sim,h_e/\sim\}$ as follows:

- $\Sigma^A=\{\epsilon\}$,
- $\rightarrow_e^A/\sim\,=\{(q,\epsilon,q')\,|\,\exists\sigma\in\Sigma,(q,\sigma,q')\in\rightarrow_e/\sim\}$.

Proposition 5.2: $\mathcal{T}_e^A/\sim$ is a bisimulation quotient of $\mathcal{T}_e^A$.

Parallel to our solution to Prob. 5.1, we construct a FSA $\mathcal{A}$ corresponding to specification formula ϕ, and then we take the product $\mathcal{PA}^A=(S_{\mathcal{PA}}^A,S_{\mathcal{PA}0}^A,\Sigma^A,\rightarrow_{\mathcal{PA}}^A,F_{\mathcal{PA}}^A)$ between $\mathcal{T}_e^A/\sim$ and $\mathcal{A}$ as described in Def. 5.2. Note that $\mathcal{PA}^A$ is non-deterministic as $\mathcal{T}_e^A/\sim$ is non-deterministic.

We formulate the fixed point problem:

$$J(s_{\mathcal{PA}})=\min(J(s_{\mathcal{PA}}),\max_{s_{\mathcal{PA}}\rightarrow_{\mathcal{PA}}^A s'_{\mathcal{PA}}}J(s'_{\mathcal{PA}})+1),\quad(16)$$

initialized with $J(s_{\mathcal{PA}})=\infty$ for all $s_{\mathcal{PA}}\in S_{\mathcal{PA}}^A\setminus F_{\mathcal{PA}}^A$ and $J(s_{\mathcal{PA}})=0$ for all $s_{\mathcal{PA}}\in F_{\mathcal{PA}}^A$.

Proposition 5.3: Let $S_{\mathcal{PA}}^{AS}=\{s_{\mathcal{PA}}\in S_{\mathcal{PA}}^A\,|\,J(s_{\mathcal{PA}})<\infty\}$ and define $\mathcal{X}^{AS}=\{\text{eq}(q)\mid(q,s)\in(S_{\mathcal{PA}0}^A\cap S_{\mathcal{PA}}^{AS})\}$. Then $\mathcal{X}^{AS}$ solves Prob. 5.2.

Example 5.3: For specification ϕ as in (13), we obtained the solution to Prob. 5.2. $\mathcal{X}^{AS}$ and sample trajectories are shown in Fig. 4. Note that this is a subset of the set of initial states found for the synthesis problem (see Fig.3).

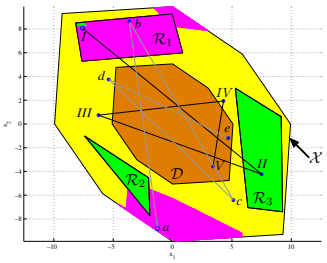


Fig. 4: $\mathcal{X}^{AS}$ is shown in purple. $\mathcal{X}$, $\mathcal{D}$, $\{\mathcal{R}_i\}_{i\in R}$ and two sample trajectories are indicated by labeling.

VI. Conclusions

We presented a method to abstract the behavior of a switched linear system within a positively invariant subset of $\mathbb{R}^n$ to a finite transition system via the construction of a bisimulation quotient. We employed polyhedral Lyapunov functions to guide the partitioning of the state space and showed that the construction requires polytopic operations only. We showed how this method can be used to synthesize switching sequences and to verify the behavior of the system under arbitrary switching from specifications given as scLTL formulas over polytopic subsets of the state space.

References

[1] R. Milner, *Communication and Concurrency*. Prentice-Hall, 1989.

[2] M. C. Browne, E. M. Clarke, and O. Grumberg, "Characterizing finite kripke structures in propositional temporal logic," *Theoretical Computer Science*, vol. 59, no. 1-2, pp. 115–131, 1988.

[3] P. Tabuada and G. J. Pappas, "Linear time logic control of discrete-time linear systems," *IEEE Transactions on Automatic Control*, vol. 51, no. 12, pp. 1862–1877, 2006.

[4] A. Chutinan and B. H. Krogh, "Verification of infinite-state dynamic systems using approximate quotient transition systems," *Automatic Control, IEEE Transactions on*, vol. 46, no. 9, pp. 1401 –1410, 2001.

[5] R. Alur and D. L. Dill, "A theory of timed automata," *Theoretical computer science*, vol. 126, no. 2, pp. 183–235, 1994.

[6] B. Yordanov and C. Belta, "Formal analysis of discrete-time piecewise affine systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 12, pp. 2834 –2840, 2010.

[7] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 116 –126, 2010.

[8] M. Lazar, "On infinity norms as Lyapunov functions: Alternative necessary and sufficient conditions," in *IEEE Conference on Decision and Control*, Atlanta, GA, 2010, pp. 5936–5942.

[9] X. C. Ding, M. Lazar, and C. Belta, "Formal abstraction of linear systems via polyhedral Lyapunov functions," in *IFAC Conference on Analysis and Design of Hybrid Systems*, Eindhoven, The Netherlands, June 2012, to appear.

[10] C. Sloth and R. Wisniewski, "Verification of continuous dynamical systems by timed automata," *Formal Methods in System Design*, vol. 39, pp. 47–82, 2011.

[11] E. Aydin Gol, D. Xuchu, M. Lazar, and C. Belta, "Finite bisimulations for switched linear systems," 2012, available at http://arxiv.org/abs/1208.5471.

[12] Z. P. Jiang and Y. Wang, "A converse Lyapunov theorem for discrete-time systems with disturbances," *Systems & control letters*, vol. 45, no. 1, pp. 49–58, 2002.

[13] M. Lazar, "Model predictive control of hybrid systems: Stability and robustness," Ph.D. dissertation, Eindhoven University of Technology, 2006.

[14] J. Bochnak, M. Coste, and M. F. Roy, *Real algebraic geometry*. Springer Verlag, 1998, vol. 36.

[15] O. Kupferman and M. Y. Vardi, "Model checking of safety properties," *Formal Methods in System Design*, vol. 19, pp. 291–314, 2001.

[16] E. M. Clarke, D. Peled, and O. Grumberg, *Model checking*. MIT Press, 1999.

[17] T. Latvala, "Efficient model checking of safety properties," in *In Model Checking Software. 10th International SPIN Workshop*. Springer, 2003, pp. 74–88.